Cassandra Crossing/ Tor, lezioni di teoria 4

(99)—Marco Calamari prosegue il suo excursus sulle tecnologie di anonimizzazione. Dopo aver compreso cosa è Tor e come si usa, e con…

Cassandra Crossing/ Tor, lezioni di teoria 4

Figure 1:

(99)—Marco Calamari prosegue il suo excursus sulle tecnologie di anonimizzazione. Dopo aver compreso cosa è Tor e come si usa, e con quali tutele e cautele, ora è il momento di vedere come contribuire al suo funzionamento.

9 novembre 2007—Fino ad ora abbiamo considerato l'uso di Tor solo come applicazione (in gergo "client"), e descritto e risolto alcuni problemi elementari che possono compromettere l'alto livello di sicurezza e privacy ottenibile con il suo utilizzo.

La rete Tor non è simile alle reti paritetiche P2P in cui tutti nodi sono uguali. I client Tor per funzionare non si connettono tra di loro ma devono obbligatoriamente connettersi a dei server, o più propriamente a dei "router" Tor.

I Router Tor non stanno lì fuori nella Rete perché ce li mettono i provider; il mestiere dei provider è fare business e l'anonimato, come anche la vicenda di Zero Knowledge ha dimostrato, non lo è. Non li ha nemmeno prescritti il medico e non sono nati sotto i cavoli. C'è qualcuno che ha deciso di metterceli e di fare anche la fatica di farceli restare.

Infatti, anche se tendiamo a dimenticarcelo, in Rete tutte le cose interessanti (ed anche quelle meno interessanti o decisamente brutte) ci sono perché qualcuno ce le ha messe, spesso volontariamente e senza essere pagato, anzi investendo il proprio tempo ed i propri soldi.

Molti navigatori sembrano invece convinti di avere il diritto di prendere a man bassa senza mai dare niente, o che "dare" significhi inserire qualche post demenziale in un forum o creare un blog pieno di applet ed effetti speciali e presto abbandonarlo (non me ne vogliano i miei amici blogger che ne mantengono alcuni pieni dei migliori contenuti della Rete—sono purtroppo una minoranza).

I router Tor sono come certe bestiole simpatiche, semplicissimi da installare ma difficili da mantenere, e qualche rara volta possono anche mordervi, proprio come un cucciolo. Sono semplici da installare perché se state già usando Tor per navigare, avete già installato tutto il software necessario. E' solo questione di fare un semplice cambiamento di configurazione, dopo aver controllato che il proprio PC sia sempre raggiungibile da Internet. Infatti potete "pubblicare" un router Tor solo se da Internet gli altri server possono raggiungervi. Il che vuol dire che non dovete trovarvi su una rete privata (in gergo "NATtata") e dovete avere una connessione permanente (ADSL) tariffata flat (altrimenti poveri voi!) e non filtrata.

Solo a titolo esemplificativo, risulta che la maggior parte degli utenti Telecom Italia possono essere raggiunti, mentre la maggior parte degli utenti Fastweb sono nattati e, trovandosi in una rete privata non possono essere raggiunti da Internet. "Your mileage may vary" quindi fatevi i vostri controlli.

Ma prima di parlare di questioni tecniche ci servono un pizzico di filosofia e di leggi. Davvero volete realizzare qualcosa col vostro e regalarlo agli altri, a gente che non avete mai visto e che non vedrette mai?

Perché è questo che farete; regalerete una parte della vostra ADSL e del vostro tempo ad altri sconosciuti, tra cui anche coloro che fino ad ora l'hanno regalata a voi. Benissimo, ma nel momento stesso in cui iniziate questo cammino, vi caricate anche di una responsabilità.

Un router Tor che duri poche ore o pochi giorni, oppure che si blocchi in continuazione non solo non è di nessuna utilità, ma è addirittura dannoso. Se non avete le possibilità materiali o la costanza di non stancarvi è meglio non farne di niente.

E visto che un server Tor deve stare acceso in continuazione, ne avete la possibilità? O vi piace tanto fare quei videogame per cui è necessario fare reboot in continuazione? In questo caso potrebbe essere necessario dotarvi di un secondo pc, anche senza monitor e di modestissime prestazioni.

Potete permettervi il (modesto) aumento della bolletta Enel dovuto al vostro pc sempre acceso giorno e notte? Puo' costarvi anche 50–100 euro in più all'anno. Ed avete pensato anche al rumore? Il vostro pc è in un luogo dove non arreca disturbo, nemmeno la notte?

In questo potrebbe venirvi in aiuto realizzare una PBox, Privacy Box. Trovate qui la descrizione di alcuni prototipi e qui una mail list in cui chiedere lumi in caso di difficoltà.

Bene. Se tutti queste problemi sono per voi superabili c'è un'altra questione di cui occuparsi; la più importante di tutte, l'aspetto legale. Infatti per gestire un router, ed in particolare un nodo di uscita dalla rete Tor (il tipo più utile alla rete Tor stessa) ci si deve preoccupare anche di problemi di responsabilità legali, analoghi a quelli da affrontare prima di mettersi alla guida di un motorino.

Esattamente come per le Poste e la rete autostradale, anche la rete Tor puo' essere utilizzata da malintenzionati od anche da veri e propri criminali. Regalare libertà e privacy a tutti "costringe" anche a non poter escludere nessuno, nemmeno i cattivi. Applicazioni per la privacy come Tor, infatti, possono funzionare solo se rendono impossibile qualsiasi tentativo di controllo,

localizzazione o censura, e non ammettono mezze misure. Non esiste una "privacy abbastanza buona".

O la privacy è totale o non esiste, proprio come una ragazza non può essere "abbastanza" incinta; o lo è o non lo è. Yoda sarebbe certamente d'accordo.

Chi fosse interessato a questo tipo di considerazioni può andarsi a leggere la vicenda reale di Jap, un'applicazione per la privacy che finì per essere controllata (a fin di bene?) dalla polizia tedesca. Magari avrà fatto catturare dei criminali, ma di certo non ha offerto privacy "reale" ai suoi inconsapevoli utenti.

Mettere in rete un server Tor espone a responsabilità di tipo legale. Badate bene, responsabilità, non necessariamente conseguenze. Il fatto è che ovviamente se qualcuno usa il vostro router per accedere, ad esempio, a contenuti controversi, la connessione avrà il vostro IP, e se durante un'indagine si tentasse di ricostruire all'indietro una connessione passata attraverso il vostro ipotetico router vi potrebbero essere chieste spiegazioni. A maggior ragione se il vostro router fosse di "uscita", tutte le connessioni fatte attraverso esso avrebbero come indirizzo quello della vostra ADSL.

Quanto segue è la mia opinione personale, ma come forse alcuni dei miei 22 lettori ricorderanno, io faccio l'ingegnere e non l'avvocato, quindi prendete tutto con beneficio d'inventario. Nella legislazione italiana esistono a riguardo due leggi significative, la legge Gasparri, o Testo Unico delle Comunicazioni ed il cosiddetto decreto Pisanu.

Nel loro complesso sanciscono due cose. L'obbligo di identificare gli utenti di un servizio pubblico di accesso alla Rete, e l'obbligo di conservare i log identificativi delle comunicazioni realizzate tramite il servizio stesso.

Secondo l'interpretazione letterale (e più comune) dei testi, l'obbligo di identificazione degli utenti sussiste solo per i fornitori diretti di accesso alla Rete, quali Internet provider commerciali oppure fornitori di accesso gratuito aperto al pubblico, come un bar od una palestra che regalino l'accesso wireless ai loro clienti.

Chi gestisce un router Tor tuttavia non fornisce accesso a fini di lucro o pubblico, perché non ha utenti identificabili, e perché le connessioni provengono solo da altri client o router Tor e non sono distinguibili tra loro perché criptate ed anche affasciate (più connessioni separate che diventano una sola).

Inoltre i router Tor non hanno informazioni utili per il tracciamento, normalmente non salvano i log, ed anche se li si salvasse essi non contengono di per sé informazioni utili per il tracciamento di una particolare connessione. Quindi, sempre secondo l'opinione e l'esperienza di chi scrive, l'unica conseguenza che potrebbe accadere al gestore di un router Tor è quella di ricevere da parte di una Autorità giudiziaria (di solito la Polizia Postale e delle Comunicazioni) la richiesta di fornire i dati di una certa connessione o tutti i log del server, che viene recapitata presso il domicilio del titolare dell'abbonamento ADSL da un messo oppure direttamente da personale coinvolto nelle indagini.

L'unica risposta possibile a richieste di questo tipo consiste nello spiegare che l'origine della connessione è un server Tor, che non è l'origine della connessione tracciata e che non è possibile risalire al suo originatore; eventualmente (se per maggiore sicurezza fossero stati conservati) potrebbe essere fornita la parte degli (inutili) log Tor richiesti.

Può essere utile, per rispondere "a priori" riducendo la possibilità di ricevere la richiesta, dotare i router Tor di una pagina web che spieghi l'impossibilità di fornire informazioni e ne motivi tecnicamente e legalmente le ragioni.

A conoscenza di chi scrive, questo in Italia è avvenuto poche volte (probabilmente una sola) nei parecchi anni di funzionamento di una trentina di router italiani. Ovviamente la lista del Progetto Winston Smith (pubblica, ma per postare dovete iscrivervi) è disponibile per fornire consigli e delucidazioni.

È quindi opportuno che una attività di gestione di un router Tor, attività fino ad oggi assolutamente legale in Italia, sia svolta solo da persone maggiorenni e tramite una connessione a loro intestata od intestata ad altra persona che sia assolutamente d'accordo. Questo per evitare di essere generosi sulla pelle degli altri.

Bene, spero che questa breve chiacchierata abbia chiarito le idee a molti e dato degli spunti di riflessione a parecchi. Per oggi quindi basta così e niente dettagli tecnici fino alla prossima rubrica. I frettolosi od i decisi possono comunque trovare molte informazioni sulla pagina di installazione del server sul sito Tor gestito in collaborazione da EFF e dal Progetto Tor

---

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on August 27, 2025.